DOC IT Security Evaluation Checklist: End User Responsibilities

A System End User is a DOC federal employee or contractor authorized to use DOC systems and networks to accomplish their official duties.

This checklist provides end users with a self-assessment tool, and their supervisors or Contracting Officer's Technical Representatives with a performance evaluation tool, to evaluate the level of compliance with end user's duties as established by the *DOC IT Security Program Policy and Minimum Implementation Standards* (ITSPP), Section 2.1.13, as well as the additional policy sources cited in the second column of the checklist.

This is an assessment of (name/operating unit/office)**:**		
	Self Assessment	**Assessment Date:**
	Third Party Evaluation	**Assessor** (name/title/org.):

Status Codes: **1** = Not Started **2** = In Process **3** = In Place

Performance Levels:

1 End user is aware of DOC IT security policies in place
2 End user is aware of DOC IT security policies as well as detailed procedures in place
3 End user is familiar with DOC IT security policies and detailed procedures and follows them
4 End user is familiar with DOC IT security policies and detailed procedures, follows them, and periodically tests his/her compliance (for example, using this checklist evaluation tool)
5 End user is familiar with DOC IT security policies and detailed procedures and practices them as part of a fully integrated IT security program

End User		**DOC Policy References***	**Status**	**Performance Level**
1	Complete IT security refresher training annually	ITSPP 15		
2	Read and understand all applicable use policies and other rules of behavior regarding use or abuse of operating unit IT resources;	ITSPP 4.5		
3	Know which systems or parts of systems for which you are directly responsible (printer, desktop, etc.)			
4	Know the security category of the data you handle and measures you must take to protect it.			
5	Notify the appropriate Help Desk, IT Security Officer, or supervisor of any suspected incidents in a timely manner, and cooperate in the investigation of incidents; and	ITSPP 14.7		
6	Know and abide by all applicable DOC and operating unit policies and procedures. This is especially true of the Internet Use Policy and Peer-to-Peer File Sharing Policy, which specify the end user's responsibility regarding Internet introduction of viruses, spam, spyware, and malicious codes, normally introduced into a system by a voluntary act of an end user (e.g., installation of an application, FTP of a file, reading mail, etc.)	Internet Use Policy, ITSPP Appendix I		
7	Use and distribute commercial software in accordance with copyright laws and licensing agreements.	ITSPP 5.7.1		
8	Protect DOC government information, including:	ITSPP 13		

* In addition to Section 2.1.10

End User		DOC Policy References*	Status	Performance Level
	(a) Accurately categorize and label all electronic files, hard copy printouts, and removable media (diskettes and CD-ROMs) as Sensitive but Unclassified (SBU), For Official Use Only (FOUO), U.S. Code Title or Public Law protected data, or national security classification (confidential, secret, top secret, or other designation)	ITSPP 13.2.1		
	(b) Enable audit logging on workstations and protect the logs	ITSPP 13.2.1		
	(c) Assign security categories commensurate with the information to be protected	ITSPP 13.2.1		
	(d) Make appropriate use of the following: – locked media libraries; – operator instructions for handling tampering or other incidents; – read-only safeguards; – least-privilege doctrine for information availability; and – auditing of the safeguards as appropriate.	ITSPP 13.2.1		